

TAKE CONTROL OF
**YOUR
APPLE WI-FI
NETWORK**

COVERS
802.11ac and 802.11n

by **GLENN FLEISHMAN**
\$20

Table of Contents

Read Me First	5
Updates and More	5
Basics	6
Finding the Wi-Fi Menu	7
What's New in This Edition	8
Introduction	9
AirPort Quick Start	10
Quick Troubleshooting Guide	12
Reset a Locked-up Base Station	12
Wi-Fi Network Won't Assign IP Address	14
Device Can't See Base Station Network	16
Other Troubleshooting	17
Mac Wi-Fi Iconography	18
Light Reading	20
Learn Wireless Basics.....	21
Adapters and Access Points	21
Wi-Fi Spectrum.....	22
Wi-Fi Standards and AirPort Hardware	24
Wi-Fi Gear from Apple	29
802.11n, 802.11ac, and Apple's Choices	29
AirPort Base Station Models.....	31
Adapters in Macs and iOS Devices	35
Meet AirPort Utility.....	36
View Your Network	36
Keep Up to Date	40
Plug In Your Base Station and Get Started.....	43
Unpack and Power Up	43
Connect to a New Base Station	45
Set Up a Network	48
Picture Your Scenario	48

New Network, Single Base Station	49
Extend a Network via Ethernet or Wi-Fi.....	53
Replace an Existing Base Station	56
Create Separately Named 2.4 and 5 GHz Networks	61
Configure IPv6 Networking.....	63
Pick the Right Place and the Right Channel.....	65
Spectrum Trade-offs	65
Pick Compatibility and Set a Channel.....	68
Pick the Right Place	72
Advanced Networking	80
Get a WAN Address	80
Hand Out LAN Addresses	86
Connect Your Devices.....	95
Connect in Mac OS X	95
Connect in iOS	106
Connect in Windows 8	107
AirPort Express Extras	110
Stream Audio with AirPlay	110
Share with Airfoil.....	114
Connect to Any Base Station	117
Connect Multiple Base Stations	119
Know the Basics	119
Add Access Points via Ethernet	121
Bridge Wirelessly	125
Reach Your Network Remotely.....	129
Know Your Options	129
Map Ports for Remote Access	130
Punch Through with NAT-PMP.....	137
Set a Default Host for Full Access.....	138
Access a Base Station via iCloud	139
Set Up a Shared Printer.....	141
Add a Printer with USB	141
Add a Wi-Fi Printer Using WPS	141
Add a Shared Printer in Mac OS X	142

Add a Shared Printer in Windows	144
Troubleshoot an Unavailable Shared USB Printer	145
Set Up a Shared USB Disk	146
Prepare Your Drive.....	147
View and Manage Connected Volumes.....	148
Work with Time Machine	150
Grant Access	153
Gain Access.....	154
Share Files with AirDrop	158
What Makes AirDrop Tick	158
Transfer Files with AirDrop.....	159
Secure Your Network	163
Simple Tricks That Don't Work.....	163
Use Built-in Encryption	165
Set Up Guest Networking	170
Overcome Interference	172
Do Some Basic Testing	172
Try a Solution	173
Appendix A: Configuration Files	175
Appendix B: Setting up a Software Base Station	177
Software Base Station	177
Ad Hoc Networking	181
Appendix C: Channels Explained	184
2.4 GHz Channels	185
5 GHz Channels	186
Appendix D: What and Where Is a MAC Address?	189
About This Book	192
Ebook Extras	192
About the Author.....	193
About the Publisher.....	194
Copyright and Fine Print	195
Featured Titles	196

Read Me First

Welcome to *Take Control of Your Apple Wi-Fi Network*, version 1.0, published in June 2014 by TidBITS Publishing Inc. This book was written by Glenn Fleishman and edited by Tonya Engst.

Make your Apple wireless network fast, reliable, and secure. Learn to configure the 802.11n and 802.11ac AirPort Extreme and Time Capsule base stations as well as the 802.11n AirPort Express base station with AirPort Utility 6 for Mac and AirPort Utility for iOS. Plus, get directions for setting up complex networks, adding shared printers and disks, and connecting to your network from Mac OS X, iOS, and Windows.

If you want to share this ebook with a friend, we ask that you do so as you would with a physical book: “lend” it for a quick look, but ask your friend to buy a copy for careful reading or reference. Discounted [classroom and Mac user group copies](#) are available.

Copyright © 2014 Glenn Fleishman. All rights reserved.

Updates and More

You can access extras related to this book on the Web (use the link in [Ebook Extras](#), near the end; it’s available only to purchasers). On the ebook’s Take Control Extras page, you can:

- Download any available new version of the ebook for free, or buy any subsequent edition at a discount.
- Download various formats, including PDF, EPUB, and Mobipocket. (Learn about reading on mobile devices on our [Device Advice](#) page.)
- Read the ebook’s blog. You may find new tips or information, links to author interviews, and update plans for the ebook.

If you bought this ebook from the Take Control Web site, it has been added to your account, where you can download it in other formats

and access any future updates. However, if you bought this ebook elsewhere, you can add it to your account manually; see [Ebook Extras](#).

Basics

Here are a few rules of the road that will help you read this book:

- **Links:** All blue text in this ebook is *hot*, meaning you can click (or tap) it, just like a link on the Web. If you click a link that takes you to a different part of the ebook, you can return quickly to where you were if your ebook reader offers a “back” feature. For example, if you use iBooks to read the EPUB version of this ebook, you can click the “Back to” link at the lower left. Or, if you use Preview on the Mac to read the PDF version of this ebook, you can choose Go > Back or press Command-[-].
- **Menus:** Where I describe choosing a command from a menu in the menu bar, I use an abbreviated description that puts the name of the menu ahead of the command. For example, at the end of the previous paragraph, “Go > Back” means “choose the Back command from the Go menu.”
- **System Preferences:** I sometimes discuss settings in System Preferences that you may want to adjust. To open System Preferences, click its icon in the Dock or choose System Preferences from the Apple  menu. When the System Preferences window opens, click the icon of the pane whose settings you want to change.
- **Path syntax:** I occasionally use a *path* to show the location of a file or folder in the Mac’s file system. For example, AirPort Utility gets installed into the Utility folder, which is in the Applications folder. The path to AirPort Utility is [/Applications/Utilities/AirPort Utility](#).

- **Mac OS X versions:** I often mention features specific to a particular version of Mac OS X, which Apple usually refers to by their “big cat” and “California” names:
 - Yosemite: 10.10 (public release planned for late 2014)
 - Mavericks: 10.9
 - Mountain Lion: 10.8
 - Lion: 10.7

My focus in this book is 10.9 Mavericks, though you’ll find some information about the other Mac OS X versions listed above.

- **Configuring a base station:** Throughout the book, I refer to using a program called AirPort Utility to configure a base station. In almost all cases, to configure a base station in AirPort Utility 6 for Mac or in AirPort Utility for iOS, you select the base station in the AirPort Utility graphical display and then click or tap the Edit button that appears. (You may have to enter a password for the base station first.)

Finding the Wi-Fi Menu

The Wi-Fi  status menu appears near the right of the menu bar on a Macintosh. It’s icon normally looks like a fan (**Figure 1**). If yours isn’t showing, you can turn it on via a checkbox in the Network system preference pane, in the Wi-Fi view.



Figure 1: The Wi-Fi status menu appears near the right of the menu bar. I’ve put a red rectangle around it, so you can spot it easily.

if you see a different fan icon marking your menu, read [Mac Wi-Fi Iconography](#) to learn what that icon means.

What's New in This Edition

This is a fresh book in some ways, but it has a hoary history that dates back about a dozen years, making it the fourth “edition” in a line of books about wireless Apple networks.

Whenever Apple has made significant changes to Mac OS X, iOS, AirPort Utility, or base station hardware, I’ve first covered those changes by revising the current edition of the book, but sooner or later the changes become so great that I’ve needed to not only thoroughly overhaul the manuscript but also rename the book. (For example, the previous title, *Take Control of Your 802.11n AirPort Network*, was unsuitable once Apple introduced its 802.11ac base stations in 2013.)

In the process of creating a new edition, I’ve swept out details about some older gear and software, so if you’re approaching wireless networking afresh, you aren’t overwhelmed with history.

This 1.0 version of *Take Control of Your Apple Wi-Fi Network* adds content about iOS 7, OS X 10.9 Mavericks, and Windows 8.1, and more fully incorporates Apple’s 802.11ac AirPort Extreme and Time Capsule, both released in early 2013. It still covers the 2012 AirPort Express, and I’ve retained some backward-looking information for the 802.11n base stations from 2008–2012, and have kept details about using Wi-Fi with 10.7 Lion and 10.8 Mountain Lion.

Note: With respect to AirPort networking, 10.10 Yosemite, by all accounts, will be nearly identical to Mavericks. I have noted a couple of exceptions in the text.

Finding an Old Edition

For help with an older version of Mac OS X, iOS, or Windows, with older base station gear, or with an older version of AirPort Utility, you can refer to a previous edition of this ebook—there’s no extra charge. Follow the “access extras” link in [Ebook Extras](#), and look in the blog.

Introduction

It's never been easier in Apple's 15-year history of offering wireless networking equipment to set up a Wi-Fi base station and start working. But if that's so, why read a book on the topic?

Even though set up is much, much easier than ever—especially with more powerful and sophisticated radio gear in the base stations—so many of the fine details of creating a network that does precisely what you want still require carefully plotted, step-by-step guidance. This is especially the case for networks with multiple base stations, attached disks, and sensible encryption.

In this book, I provide you with tips to save time, improve security, extend range, and enjoy a technical edge when working with Wi-Fi.

I start with wireless basics, move through base station installation and configuration, explain how to share printers and hard disks, tell you how to connect to a Wi-Fi network, give advice on extending a network's range and quality, look at using an AirPort Express's unique features, and finish with how-to information on security for those who want their AirPort networks safe from freeloaders and intruders.

AirPort Quick Start

Use this Quick Start to get an idea of how you might jump into the book if you are at a particular stage in working with your network.

Tip: Trying to solve a problem? Flip ahead a few pages to the [Quick Troubleshooting Guide](#) or see [Light Reading](#) to learn what the light on your base station is trying to tell you. Also, you may especially wish to consult [Overcome Interference](#).

Learn wireless basics:

- Get a quick grounding in [Learn Wireless Basics](#).
- Familiarize yourself with [Wi-Fi Gear from Apple](#).

Plan your network:

- For common configurations, see [Picture Your Scenario](#) and focus on the diagrams and descriptions at the beginning of: [New Network](#), [Single Base Station](#), [Extend a Network via Ethernet or Wi-Fi](#), and [Replace an Existing Base Station](#).
- For ideas on using the AirPort Express, skim [AirPort Express Extras](#).
- For more advanced possibilities, consult [Connect Multiple Base Stations](#) and pay special attention to the descriptions and diagrams at the start of [Add Access Points via Ethernet](#) and [Bridge Wirelessly](#). Also, note that Appendix B covers creating a [Software Base Station](#) and [Ad Hoc Networking](#).
- Although it's not necessary for a basic setup, you can consider the channels and bands that your Wi-Fi network will use in [Spectrum Trade-offs](#).

Set up your base station(s):

- You'll be using AirPort Utility to configure your base station. Read [Meet AirPort Utility](#) to learn the basics.

- Unpack your base station and start down the path of configuring it in [Plug In Your Base Station and Get Started](#).
- Share a printer or a hard drive. See [Set Up a Shared Printer](#) or [Set Up a Shared USB Disk](#).
- Set up Time Machine backups with an AirPort Extreme or Time Capsule in [Work with Time Machine](#).

Connect to your base station:

- Find out how to connect Macs, iOS devices, and Windows systems to a base station in [Connect Your Devices](#).
- Access your network when you're not physically on it. See [Reach Your Network Remotely](#).
- Access your base station with the Back to My Mac service in iCloud. See [Access a Base Station via iCloud](#).

Add audio:

- Stream audio (and video) through AirPlay. See [Stream Audio with AirPlay](#) and [Share with Airfoil](#).

Connect between devices:

- Try AirDrop peer-to-peer file transfer in [Share Files with AirDrop](#).

Secure your network:

- Avoid [Simple Tricks That Don't Work](#).
- Apply encryption using the best—and often simplest—method. See [Use Built-in Encryption](#).
- Let visitors and friends in, when you [Set Up Guest Networking](#).

Learn still more advanced topics:

- Stop pulling your hair out over a problem with new firmware you install that doesn't work. See [Reverting to Older Firmware](#).
- Get a few details about saving and re-using an AirPort base station's settings in [Appendix A: Configuration Files](#).

Quick Troubleshooting Guide

If you need quick help, here's the starting point. I first look at handling a locked-up base station and then give tips for solving a variety of common problems.

Note: [Light Reading](#), a few pages ahead, helps you learn about a problem by decoding a base station's LED status light.

Reset a Locked-up Base Station

If an AirPort Extreme, AirPort Express, or Time Capsule appears neither in the Wi-Fi  menu as an available network nor in AirPort Utility as an available base station, or AirPort Utility identifies it as missing, try these steps in order:

Check a Local Connection

Make sure that the computer running AirPort Utility is on the same local network as the base station. Try connecting the computer via Ethernet to one of the base station's LAN ports. Try AirPort Utility again.

Cycle the Power

If a direct Ethernet connection doesn't work, try cutting the power.

Before you turn off a Time Capsule, make sure Time Machine backups or other transfers aren't in progress—for each computer on your network that uses the Time Capsule, eject any mounted Time Capsule volumes and halt Time Machine backups. The easiest way is via the Time Machine system preference pane: flip On to Off. After you power cycle the Time Capsule, you can flip Time Machine back on for each computer.

Remove the power adapter's plug from the wall socket or remove the end that plugs into the base station. Wait 10 seconds. Plug the base station back in, and see if it appears in AirPort Utility. Everything may be back to normal.

Reset the Base Station

If the above two options don't work, then try a reset.

This step may erase any custom settings you've made. Straighten an end of a paperclip, and with the base station plugged into power, hold down the base station's reset button with the paperclip tip for about 5 seconds until the status light turns amber and flashes rapidly. Release the button and wait a minute or so for the base station to restart.

Three Kinds of Reset

Apple has [an extremely detailed FAQ](#) about base station resets that's worth reading if you have problems. But the crucial thing to know is that there are three kinds of resets on all 802.11n and 802.11ac base stations. There's a tricky bit here! The difference between a *hard* reset and a *factory* reset is the state of the device—not how long you hold down the button! Read on:

- ✦ **Soft reset:** Hold reset for 1 second, and the base station disables passwords and network security for 5 minutes, during which time you may change settings, including passwords. AirPort Utility indicates the device is in a "soft reset" state, and its LED flashes amber.
- ✦ **Hard reset:** Hold reset for 5 seconds, and the base station flashes its LED rapidly in amber, and then restarts. While it boots up in a clean, factory state, it also stores your previous settings. To restore those settings, click Other Wi-Fi Devices in AirPort Utility (at the upper left of the main AirPort Utility for Mac screen), click Other Options, select Restore Previous Settings, and then click Next on subsequent screens.
- ✦ **Factory reset:** If a base station is truly crashed and cannot boot, its firmware knows! Hold reset for 5 seconds, and the base station reboots like in a hard reset, but your previous configuration is lost.

Mac Wi-Fi Iconography

The Wi-Fi menu—located on the system menu bar—reveals what kind of connection is in progress on your computer. Knowing what the icons mean can help you troubleshoot problems. This icon is always at the top of the Wi-Fi menu.

Note: If you don't see a Wi-Fi menu on the system menu bar, read [Finding the Wi-Fi Menu](#), earlier.



A gray fan indicates an active Wi-Fi network adapter that isn't currently connected to a network. Read [Connect Your Devices](#).



A full fan with one or more black bars—the bars represent current strength—indicates a current Wi-Fi connection to either a base station or a network created through the Sharing system preference pane's Internet Sharing service. (An animation of each wave turning black in turn occurs while the connection is underway.) For more information, consult [Connect Your Devices](#) and [Appendix B: Setting up a Software Base Station](#).



iOS devices may share a cellular connection via Wi-Fi using the Personal Hotspot feature. When a Mac connects to such a network, the fan icon is overlaid with interlinked loops. Apple also uses this symbol in iOS to indicate a tethered connection of this kind.



A fan showing an up arrow indicates that the Internet Sharing service is active on this computer. See [Software Base Station](#).



A fan containing a computer shows that the Mac has created an *ad hoc network*, a method of handling Wi-Fi communication among multiple computers without a base station—not even the “software” base station that’s created by Internet Sharing. See [Ad Hoc Networking](#), in Appendix C.



A fan containing an exclamation point indicates an error in setting up the network part of the Wi-Fi connection. Although the computer has connected wirelessly to the base station, it was unable to obtain a network address. See [Wi-Fi Network Won’t Assign IP Address](#).



An empty fan outline indicates that either there’s no Wi-Fi adapter in the computer, or the Wi-Fi adapter is off. To turn it on, choose Turn Wi-Fi On from the menu. If the Wi-Fi icon still looks like an empty fan or an error says that there’s no card or it can’t be turned on, you may have a hardware problem.



The Eye of Sauron appears in its unblinking form that sees all and knows all when you use a monitoring mode in Wireless Diagnostics, a hidden tool that can help you sort through problems. See [Run Wireless Diagnostics](#) for more details.

Light Reading

The light on the front of any Apple Wi-Fi base station indicates what the base station is up to: handling data correctly, hitting an error, or in a special mode. The guide below helps you decipher the meaning:

- **Off:** There's no power! Plug in the base station. If it is plugged in, check that the wall outlet is putting out power (you can plug a lamp into the outlet to test this). If the wall outlet is putting out power, try methodically disconnecting and reconnecting any plugs between the base station and the wall in order to determine whether the problem is a loose connection or a broken cable (or power strip, UPS, or other intermediary device).
- **Blinking green:** The light blinks or flashes green in two cases:
 - **Startup:** The light flashes green on and off for 1 second.
 - **Reset:** This happens after you press the recessed reset button for long enough to trigger a reset.
- **Solid green:** The base station is configured correctly, has no updates available, and is connected to the Internet.
- **Solid amber:** The base station is still powering up and hasn't loaded all its settings and connected to the network.
- **Slowly blinking amber:** This light has several meanings:
 - The base station has a configuration problem, has lost its network connection, or is suffering from another problem. Use AirPort Utility to troubleshoot the problem.
 - You just did a soft reset, and the base station is in the 5-minute period when its access and network passwords are disabled.
 - A Time Capsule may have a [Disk Integrity](#) problem.
- **Rapidly blinking amber:** You just did a hard reset (or a factory reset). The base station is modifying its settings before it restarts.

Learn Wireless Basics

Let's quickly run through some basics to set the stage for what follows.

Adapters and Access Points

Wi-Fi networks need two connected parts: a wireless adapter and an access point. The *wireless adapter* is part of a computing device (such as a desktop computer, tablet, or smartphone), while the *access point* connects both to wireless adapters and to a broader network, such as the Internet via a broadband modem. An access point that's coupled with a router is called a *wireless gateway*; Apple calls its wireless gateway a *base station*.

Apple's lineup of base stations includes the AirPort Extreme, the AirPort Express, and the Time Capsule. When I talk about "AirPort equipment," I mean all Apple base stations, including Time Capsules.

An *AirPort network* is a Wi-Fi network with some Apple extras that may work only with Apple software—under Mac OS X or Windows—or in conjunction with other AirPort equipment. Examples of such features include streaming audio, certain forms of hard-drive file sharing, and base-station-to-base-station connections.

What's Wi-Fi?

The name *Wi-Fi* is a certification guarantee for which the Wi-Fi Alliance trade group owns the rights and controls the testing. *Wi-Fi* doesn't stand for anything—it's a made-up name—but it loosely connotes *wireless fidelity*, in the sense of *faithfulness*: devices with Wi-Fi stamped on them work with other Wi-Fi devices following the same standards, or are faithful to one another.

The wireless adapter uses client software on the device to connect to a specific base station (or set of affiliated base stations) after a user selects the network name from a list or manually enters the network name. (For example, in Mac OS X you can choose a network from the

Wi-Fi  menu in the menu bar and the Wi-Fi view in the Network system preference pane.)

When a device's wireless adapter connects—technically, *associates*—with a base station, the device can send data to and receive data from the base station. If the base station has encryption enabled, then the device must provide an encryption key before the base station allows the device access to any networks to which it connects. The key, which consists of a series of characters, needs to be provided exactly as it was entered on the base station, whether typed or tapped in or sent from a keychain in the operating system.

Once an adapter connects to a base station and the encryption key is accepted, the device's operating system can carry out the next steps, such as automatically requesting an Internet protocol (IP) address using DHCP and sending data over the wireless network.

With newer adapters, a connection may be made directly to another device with peer-to-peer networking regardless of whether the adapter is connected to a regular Wi-Fi network. An example is AirDrop, an Apple-only version of a more general standard called *Wi-Fi Direct* (see [Share Files with AirDrop](#)).

Wi-Fi Spectrum

Wi-Fi networks use *unlicensed spectrum*, so called because regulatory agencies allow license-free use of those airwaves by everyone in a given country. In contrast, cellular telephone companies pay huge amounts for the exclusive geographic rights to certain frequencies.

Note: In some developing nations, inexpensive or free licenses are required for outdoor use but not indoor use, or by businesses but not individuals. In the United States, Australia, Japan, South Korea, and most of Europe, no licenses are required.

Spectrum *bands*—specified ranges of frequencies—are divided into smaller portions called *channels*, which allow many devices to use

Wi-Fi Gear from Apple

A long history with Wi-Fi has led to three devices in Apple's current lineup of base stations, each with a distinct set of features. Let's look first at how Apple has chosen to work with 802.11n and 802.11ac, and then at Apple's current [AirPort Base Station Models](#) and the options for [Adapters in Macs and iOS Devices](#).

At the end of this chapter, you should better understand the gear that you have, or be in a better position to shop for new equipment.

802.11n, 802.11ac, and Apple's Choices

Apple has made distinct choices when implementing Wi-Fi, but all three of Apple's current base station models can handle both the 2.4 GHz band and the 5 GHz band at the same time.

Note: Despite the AirPort Express being called an 802.11n base station and the 2013 models of the AirPort Extreme and Time Capsule's being labeled 802.11ac, these are really "multi-protocol" devices. That is, the Express can handle a, b, g, and n in any combination; the 2013 Extreme and Time Capsule handle a, b, g, and n while *also* adding ac in the 5 GHz band.

For the 5 GHz band, Apple enables just 8 of the 23 possible channels in the United States for use in a base station. This is because of a compromise among the radio equipment industry, the military, government agencies, and the FCC. This compromise protects 15 of the possible 23 channels so that base station signals don't cause even the slightest interference with weather-sensing and military radar, but it also makes it more difficult to use those channels for home networks. Apple has chosen not to support those 15 channels in its base stations. The company doesn't think that they would be consistently available in a way that would be useful to most consumers and small offices using AirPort gear.

Note: The adapters in a Mac can, in fact, connect to all the 23 legal channels in the United States. Some companies may deploy Wi-Fi networks using non-Apple base stations that allow the use of all 23 channels, as they're more likely to be available inside buildings without hitting military and weather radar rules.

Note: In March 2014, the FCC voted to add another 100 MHz for unlicensed wireless use, about five channels' worth, in the 5 GHz without the same sort of restrictions that have plagued the 15 channels noted above. However, it is almost certain that no existing 802.11ac or n hardware will work in that new band. We may be waiting for some time before those are available in practical terms.

Apple also chose to limit 802.11n's wide channels to the 5 GHz band. *Wide channels* are an 802.11n feature that uses two adjacent channels at once—this doubles the raw bandwidth. Apple's choice was an option under the Wi-Fi Alliance's certification rules, but some vendors offer wide channels in 2.4 GHz.

In practice, 2.4 GHz wide channels don't work well, because 802.11n devices tread lightly to avoid interfering with other networks. In a real-world situation, you would likely see an improvement in throughput with 2.4 GHz wide channels only if no other Wi-Fi networks were nearby.

Even wider channels are possible in 802.11ac: the equivalent of four and eight normal channels in 5 GHz, the only band in which 802.11ac functions. Apple supports only the four-channel-wide flavor, which makes sense as there aren't eight adjacent channels available for consistent use in 5 GHz.

Meet AirPort Utility

AirPort Utility is an app from Apple designed to help you configure your Apple base station, troubleshoot certain network problems, and apply any available firmware updates to an Apple base station. Before you set up your base station, skim the information here about viewing your network, and then follow the advice about keeping up to date.

In this chapter, I talk about AirPort Utility 6 for Mac and AirPort Utility for iOS.

AirPort Utility 6 for Mac runs in 10.7.5 Lion and later. My directions for AirPort Utility should work identically in Lion, Mountain Lion, and Mavericks, but they've been specifically tested in Mavericks. (See [Finding an Old Edition](#), earlier, for more about AirPort Utility for Windows and older versions of AirPort Utility.)

AirPort Utility for iOS is still on version 1, and it runs in iOS 6 and iOS 7. AirPort Utility should work the same in iOS 6 and 7, but my advice in this book has been tech edited for iOS 7.

Note: On a Mac, you can launch AirPort Utility from [/Applications/Utilities](#). In iOS, first download [AirPort Utility](#) from the App Store (it's free), and then tap its icon to launch it.

View Your Network

AirPort Utility uses a graphical display of your network's *topology*, the interconnection among its networked parts, to show which base stations are available and their respective statuses.

For example, in **Figure 4**, AirPort Utility shows that AirPortage Bay is connected to the Internet, while Downstairs AirPort and Guest Room Apr2011 connect via AirPortage Bay for their network needs. (They look to AirPortage Bay for DHCP and NAT address handling.)

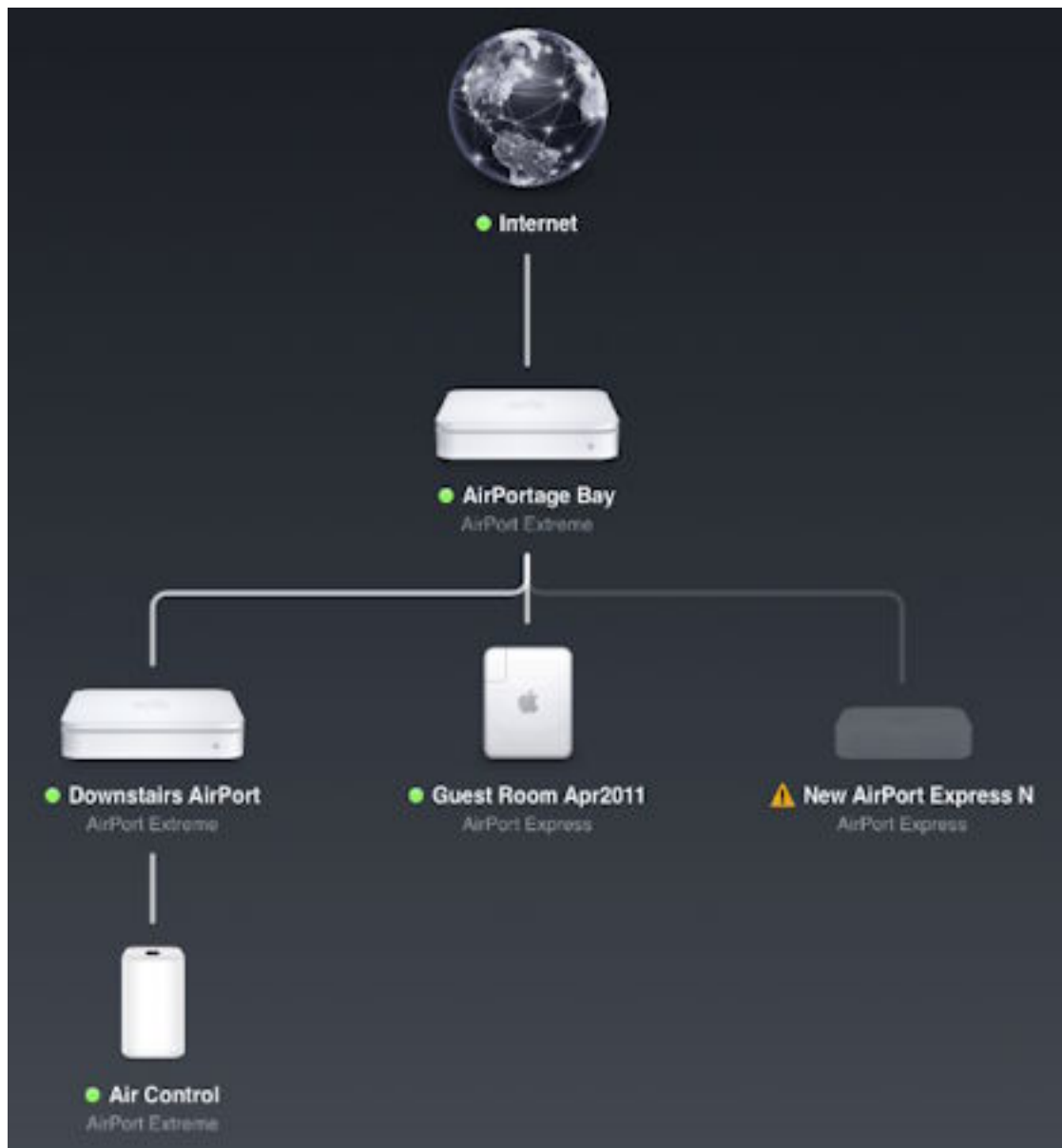


Figure 4: AirPort Utility offers a graphic depiction of your network and its interconnections.

The topology represents Ethernet connections with solid lines and wireless connections with dotted lines (**Figure 5**).

Plug In Your Base Station and Get Started

Let's get unpacking! This chapter focuses on plugging in your base station and on launching AirPort Utility, the program that modifies a base station's settings.

(The next chapter, [Set Up a Network](#), helps you determine which network type you want to use your base station with, and provides specific instructions for a streamlined setup.)

Unpack and Power Up

Unpack the base station to determine what you have and if you need any additional hardware:

1. **Remove the base station from its box and check the parts:**
The box includes just a few necessary parts: the base station, a setup booklet, a booklet full of software licensing information (extraneous for users, but required), and an AC power cord.
2. **Do you need an Ethernet cable?** Configuring a base station may be simpler if you temporarily hook it to a computer or existing LAN with an Ethernet cable, instead of making a wireless connection, so consider an Ethernet connection for setup.

Also, in the likely case that you plan to connect the base station to a broadband router or other network, you will need at least one Ethernet cable in order to make that connection.

3. **Is the power cord long enough?** Plan to buy an extension cord if the included 6.5 foot/2 meter cord is too short for your purposes. The Extreme and Time Capsule work best level on a table or floor, where the top of the unit has an unobstructed line of sight to the rest of the room. If you can, don't put it inside a cabinet or behind a

computer. (For now, your goal is to plug the base station in where you can set it up, though you may wish to skip ahead and read [Pick the Right Place](#) before you continue.)

Now it's time to power up. Plug your base station into an electrical outlet, and plug an Ethernet cable from your Mac into any of the three LAN ports on the Time Capsule or Extreme, or the single LAN Ethernet port on the Express. You can also plug in a base station via Ethernet to a switch or base station on the network to which your computer or iOS device is connected. If you'd rather have mobility while configuring, you can set up via Wi-Fi, but you must reconnect after each time you change password or naming options.

In a neat addition, each Ethernet port on a base station has a tiny green LED that lights up when an Ethernet cable is connected to the port and a live connection is on the other end of the cable; the LED flashes to indicate activity (**Figure 11**).



Figure 11: A very, very tiny green LED inset into the Ethernet port glows to show an active Ethernet connection and flashes on traffic.

Note: A green/amber LED on the front of the base station shows the status of the base station. [Light Reading](#), earlier, has more about the front LED.

I recommend not connecting a base station via the WAN (Wide Area Network) port to a broadband modem or the rest of your network until you've carried out more of the setup, especially the very next part.

Set Up a Network

In this chapter, I look at *scenarios*: pairing the kind of network that you want with an explanation of how to use AirPort Utility for a basic configuration of that scenario. (At the end of this chapter, I talk about two special options, [Create Separately Named 2.4 and 5 GHz Networks](#) and [Configure IPv6 Networking](#). Most people can skip these topics.)

The next chapter helps you tweak your selection of channels and determine exactly where to place your base station.

Placing a Base Station

If you haven't figured out where best to put your new base station or stations, you may wish to skip ahead and read [Pick the Right Place](#). Note that you can configure a base station first, and then relocate it, using advice in that section to find the optimal placement.

Picture Your Scenario

Pick a scenario and proceed as directed; each scenario begins with a diagram and explanation of the type of network and then gives steps.

Are you:

- Setting up a new network with a single base station connected to a broadband modem? See [New Network, Single Base Station](#).
- Extending a network? See [Extend a Network via Ethernet or Wi-Fi](#).
- Replacing an existing base station with a new unit and want exactly the same settings? See [Replace an Existing Base Station](#).
- None of the above. If your scenario isn't in this list, consult later sections in this book, which examine advanced options.

New Network, Single Base Station

In the simplest setup, where you have a single base station and are connecting it directly to a broadband modem (Figure 15), you can breeze through setup.

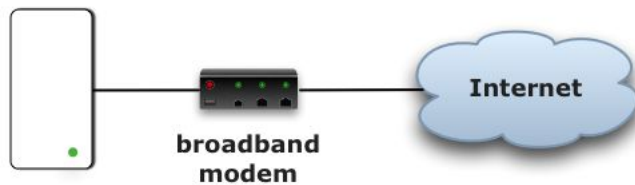


Figure 15: A simple network connects a base station via a broadband modem to the Internet.

To configure a new base station to create a new Wi-Fi network:

1. On the Mac or in iOS, select the base station as described in [Connect to a New Base Station](#), previous chapter.

AirPort Utility (or AirPort Setup in iOS) shows its progress while it gathers information (Figure 16).



Figure 16: AirPort Utility for Mac gathers information.

2. Since there are no other base stations to which you're connected, wait until you see "This *base station type* will create a network." Then, click the Next button to get a screen where you can fill in the details about your new network (Figure 17) and (Figure 18).

Pick the Right Place and the Right Channel

This chapter helps you tune your network for optimum performance. It starts by helping you understand more about the portion of the radio frequency spectrum that your base station uses and how to determine the right channel to use in each frequency band. After that it explains how to [Pick Compatibility and Set a Channel](#).

Finally, you'll learn how to [Pick the Right Place](#) for a base station with [General Testing Advice](#) as well as details on [Testing from Client to Base Station](#) and [Testing from Base Station to Client](#).

Note: Apple added simultaneous dual-band radios to the early 2009 Extreme and Time Capsule and the 2012 Express.

Spectrum Trade-offs

Shortly, I explain how to select channels for a base station. To make the best choice, you may need some background on spectrum and channel choices. (If you don't know the basics of spectrum bands and channels, read [Wi-Fi Spectrum](#) before proceeding here.)

Let's begin by comparing the two bands. The 2.4 GHz band is crowded with Wi-Fi networks, Bluetooth devices, and other uses; the 5 GHz band is relatively empty—in the United States, the band has almost seven times the amount of frequency available in 2.4 GHz. Further, Apple restricts what were once called *wide channels* to the 5 GHz band in 802.11n in order to avoid treading on 2.4 GHz networks. These broader channels in 802.11n use twice the amount of spectrum (40 MHz) and thus can achieve twice the data throughput.

802.11ac, which functions only in the 5 GHz band, can employ quadruple-wide channels that use 80 MHz of spectrum. This extra width allows a more efficient radio encoding to boost data rates higher.

Other Uses of the 2.4 and 5 GHz Bands

The 2.4 GHz and 5 GHz bands weren't empty before Wi-Fi networking came along. 2.4 GHz is known as a "junk band" because it's full of approved uses that can conflict at times. Industrial sealers, for instance, use heating processes that emit 2.4 GHz radiation. (There are many other junk bands, too, most not used for networking.)

Problems with Wi-Fi networks often stem from your own or your neighbors' use of conflicting technology, including 2.4 GHz cordless phones, microwave ovens, nearby industrial sites, and wireless cameras. The 5 GHz band has many fewer approved uses; primarily, 5.8 GHz cordless phones will be your enemy.

Throughput

The 5 GHz band offers consistent *throughput*—the amount of actual data passing over the network exclusive of overhead used to transmit it. With 2.4 GHz, however, throughput is all over the place. When other technologies interfere in the 2.4 GHz band, Wi-Fi devices and base stations are forced to slow down.

The highest possible 802.11n rate happens when two adapters use the 5 GHz band with 40 MHz, and the highest 802.11ac rate happens with 80 MHz channels.

Note: The highest rate for 802.11n is 150 Mbps in a wide channel times the number of streams in that band. That's a minimum of 150 Mbps for single-stream devices up to a maximum of 600 Mbps for four-stream devices. With 802.11ac, it's a minimum of 433 Mbps when an 80 MHz channel is available, and up to 1.3 Gbps in an Apple device. It could be much faster in future eight-stream devices!

Advanced Networking

Did the simplified setups explained in [Set Up a Network](#) not cover everything you needed to get up and running? In this chapter, I spell out the details for connecting a base station to a WAN and for further configuring addressing on your LAN. Advanced options are needed for networks that use static or fixed addresses, and for anything the slightest bit unusual.

Note: If you're building or re-building a network with more than one base station, read this chapter first to set up the base station that connects directly to your broadband service provider. Then read [Connect Multiple Base Stations](#).

Note: To stream music to an AirPort Express with AirPlay, see [AirPort Express Extras](#).

Get a WAN Address

The more complicated scenarios start with getting a WAN address for your base station; you'll then move to LAN configuration.

To communicate with the rest of the world, you need to hook the wide area network (WAN) port of your base station either into a broadband modem or, if you have an existing Ethernet LAN to which you are connecting the base station, into that larger network (**Figure 42**).

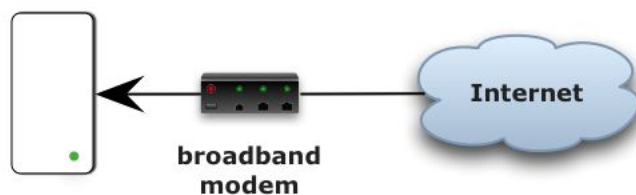


Figure 42: Plug your broadband modem into the base station's WAN port.

Start with an Ethernet cable and plug it into the WAN port on your AirPort device. Connect the other end of the cable to the LAN port of your broadband modem, or to an Ethernet switch for a larger network.

LAN vs. WAN

Connecting a broadband modem to a LAN port will not connect it to the Internet. The WAN port (**Figure 43**, left) has a circle of gray dots above it; the LAN port (**Figure 43**, right) sports a dotted line with an arrow on either end.

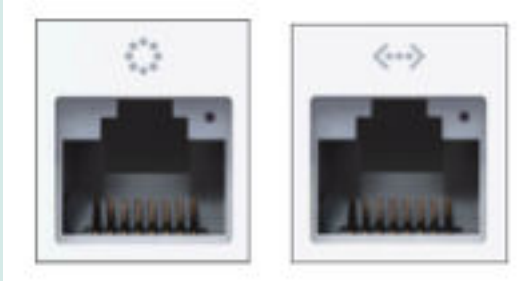


Figure 43: Left: the WAN port. Right: the LAN port.

When you make your Ethernet connection, be sure to plug the cable in to the correct port.

Now that you’ve made the physical connection, you can configure your base station to handle the connection. The many different possible configurations can be broken down into two categories: those that use *dynamic addressing* and those that use *static addressing*:

- If your Internet connection is a home broadband connection, you’ll probably use dynamic addressing; you may need to ask your ISP for more information if you’re not sure whether they provide you with a dynamic address or not. For configuration details, read “Dynamic Addressing,” next.
- A static address is more typical for small and large offices. For setup information, see [Static Addressing](#), a few pages ahead.

Dynamic Addressing

A *dynamic address* is an Internet protocol (IP) address that is assigned through Dynamic Host Configuration Protocol (DHCP), a relatively old Internet technology. With DHCP, your base station

Connect Your Devices

Once you've set up your Wi-Fi network and connected it to the Internet, you'll want to configure your devices to connect to the network properly, whether you're working in your own home or helping customers with a public hotspot.

Making a connection is quite simple, but configuring how a device connects may take a little thought. You might have a device connect automatically to unknown networks, or need to connect to a network that doesn't advertise its name. You may also want your device to automatically reconnect to networks that it has connected to before.

Read this chapter to learn how to [Connect in Mac OS X](#), [Connect in iOS](#), and [Connect in Windows 8](#).

Note: Just because a network is visible doesn't mean you can connect to it. MAC address access control and other restrictions could keep you from joining. See [Secure Your Network](#).

Connect in Mac OS X

Mac OS X regularly looks for networks, and a list of any found networks appears in the Wi-Fi  menu when the Wi-Fi adapter is on. (If it's off, choose Wi-Fi > Turn Wi-Fi On.)

Tip: If you don't see a Wi-Fi  menu on the system menu bar, read [Finding the Wi-Fi Menu](#), earlier.

If a Wi-Fi network appears nearby and your Mac isn't already connected to one (for instance, if a neighbor turns on a new network or if you open your laptop in a coffee shop), Mac OS X will alert you (**Figure 50**). From that alert, you can then connect to the network.

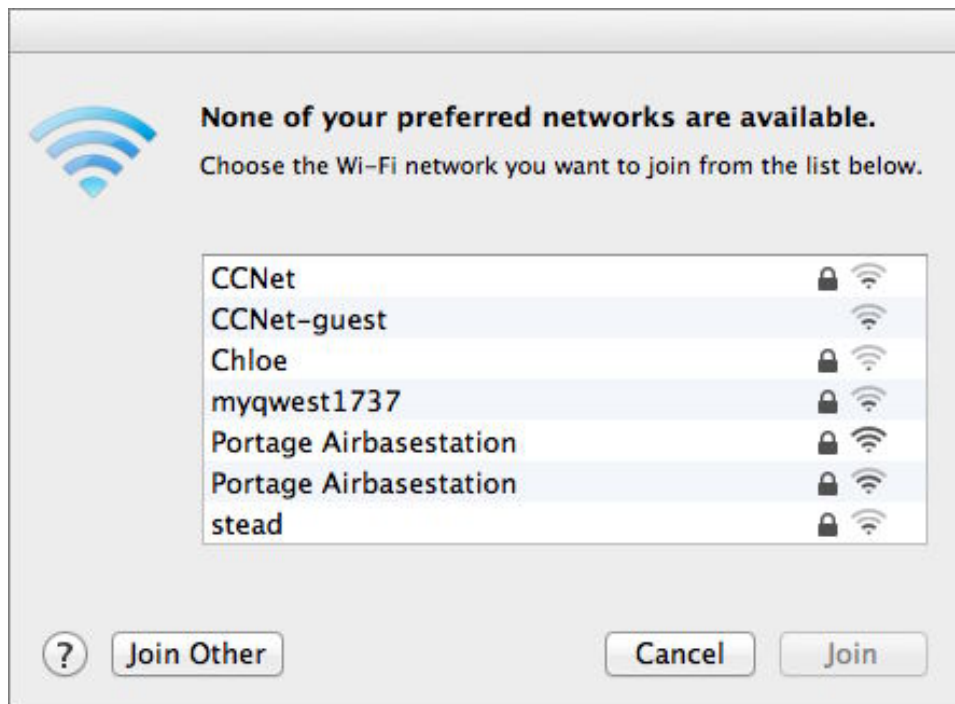


Figure 50: Mac OS X alerts you to a new network.

Your Mac will automatically join any network that it's been told to remember: it will connect when you wake it up or turn it on, when you turn Wi-Fi off and back on, when a network is turned on nearby, or even when a Wi-Fi network disappears and reappears while you're actively using the computer.

Note: The techniques described here are nearly identical to those used in Leopard and Snow Leopard.

You can also join a Wi-Fi network by choosing it from the Wi-Fi menu:

- To join a network when the network broadcasts its name—as most do—choose the network name from the Wi-Fi menu (**Figure 51**).
- To connect to a closed (hidden) network, choose Join Other Network.

AirPort Express Extras

The AirPort Express, for its modest size and price, includes several features found in neither a Time Capsule nor an AirPort Extreme, mostly around music. The Express also hides a nifty connection option for extending a network.

Stream Audio with AirPlay

AirPlay is a method of streaming media from a computer or iOS device to an external output device, such as an AirPlay-compatible speaker or an Apple TV, or—most interestingly for our purposes—an AirPort Express.

In the case of the AirPort Express, only audio can be streamed. The Express sends the stream through its audio output port (**Figure 63**) to stereo speakers. You control the settings in AirPort Utility, and then play the audio from an iOS device or from a Mac.

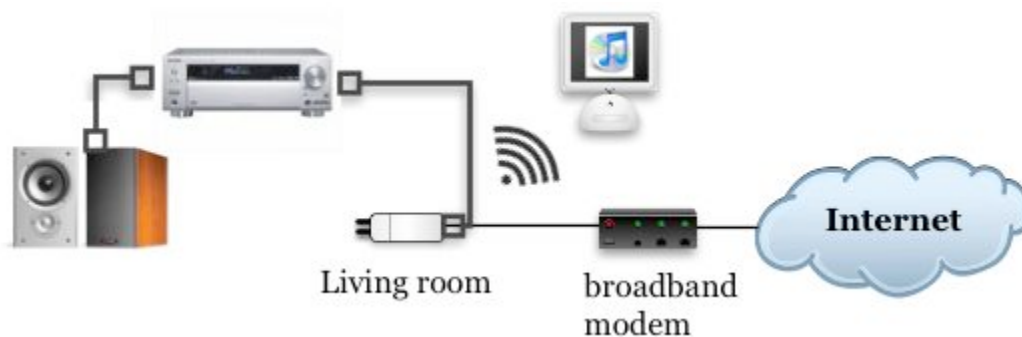


Figure 63: You can stream music from a computer on the network through AirPort Express to a stereo or powered speakers.

Note: AirPlay audio streaming works from an iPhone 4 or newer, a 4th-generation iPod touch or newer, and any iPad or iPad mini. It also works from any Mac running 10.8 Mountain Lion or later; older Mac systems can stream audio to the AirPort Express, but only from iTunes 10.2 or later.

Note: The second- and third-generation Apple TV can receive AirPlay mirroring from AirPlay-compatible iOS devices and from most moderns Macs. Read [Take Control of Apple TV](#) for more information.

Set Up AirPlay

To set up AirPlay, open AirPort Utility and edit your AirPort Express's configuration. Click or tap the AirPlay button to see the AirPlay view (the Mac version is shown in **Figure 64**).

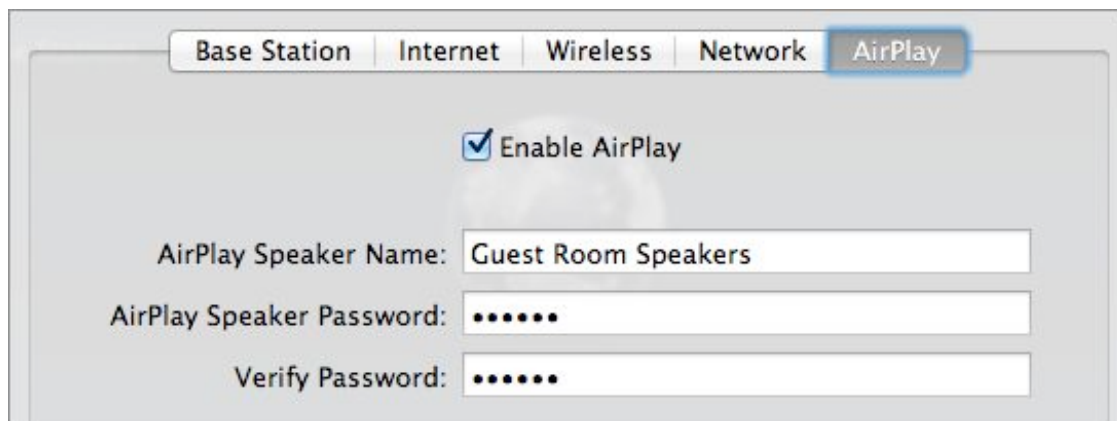


Figure 64: You can set a few AirPlay options.

Ensure that the Enable AirPlay checkbox is selected, and name your AirPlay speakers. The name appears in the Mac's remote speaker list and in the AirPlay list in iOS. You can set a password to limit use of this speaker set to people who have the password. Click Update to apply changes.

Play Any Audio from OS X

To stream audio from your Mac to an AirPlay device, open the Sound pane in System Preferences, click the Output button, and select an AirPlay option from the list of output choices—look for an AirPlay designation in the Type column. If a password is set, you are prompted to enter it. The volume on your computer controls the remote volume.

Tip: You can switch your Mac's audio output to a different device (including an AirPort Express) by pressing Option while you open the Sound menu on the menu bar and then choosing the desired device.

Connect Multiple Base Stations

Wi-Fi was once described as reaching “only” about 150 feet, which is a rough estimate of the radius of older 802.11b and g devices; with 802.11n and ac, the distance is sometimes cited as longer, or just as “farther,” because it’s impossible to characterize with any precision how Wi-Fi signals will pass through any arbitrary house, office, café, airport, or store. Also, range measured as a linear dimension misstates the problem of *volume*, the three-dimensional space to fill.

But you can extend the covered volume by adding more base stations with overlapping signals. As a Wi-Fi adapter in a device moves across overlapping regions, it can automatically switch base stations while maintaining a network connection.

Know the Basics

When you extend a network, the additional base stations tend to be dumb; that is, they don’t assign addresses or handle other features you think of as belonging to a base station. Rather, one base station remains smart, offering DHCP and NAT (if needed), among other network choices. The rest pass through traffic from that main unit. Dumb base stations are often called *access points* to distinguish them from gateways.

Because dumb base stations (access points) just pass traffic through, an adapter retains the same IP address as it switches from one base station to another, thus maintaining its connection in most cases.

There are two mix-and-match methods of extending your network:

- Add base stations via Ethernet. Ethernet requires wires, of course, but has a huge speed benefit over wireless extensions.

- Add base stations wirelessly via Wireless Distribution System (WDS). This method avoids new wires, but can have severe speed limitations in comparison to Ethernet.

I write “mix and match” because you can use any combination of Ethernet and WDS to build a network. Let’s start with the simpler case, which is to [Add Access Points via Ethernet](#). After that, there’s a sidebar about [Extending with HomePlug](#), in case you want to use your home’s electrical system in place of Ethernet. And, finally, I talk about how to [Bridge Wirelessly](#).

Create or Extend a Network

When you work in AirPort Utility to build a network of two or more base stations, connecting them with Ethernet, Wi-Fi, or a hybrid, you will need to choose an option from a pop-up menu in the Wireless View. Those options may confuse you, so let’s look at them first. For each base station, in the Wireless view's Network Mode pop-up menu, you can choose either of two options:

- ✦ Create a Wireless Network is for either a main base station in a wirelessly connected network (or pod of access points), or each base station connected via Ethernet.
- ✦ Extend a Wireless Network might seem like the right option for adding a base station via Ethernet, but it is not. Extend a Wireless Network refers only to extending wirelessly: when you connect two or more base stations with Wi-Fi, the additional base station(s) that have only a wireless connection to the network use this Extend option.

What about ProxySTA?

The ProxySTA mode of extending an existing Wi-Fi network with an Express is another method, but it has its limits: it works only with an AirPort Express, and it allows only the extension of the network via the LAN Ethernet port on the Express. In contrast, linking base stations with Ethernet and WDS creates a larger and full-featured LAN with both Wi-Fi and Ethernet connectivity.

See [Connect to Any Base Station](#), a few pages earlier, for details on ProxySTA.

Reach Your Network Remotely

When you share an Internet connection among one or more computers on a local network using private addresses, you give up having an easy way to connect from the outside world to a service, like a Web server or fileserver, that's located on one of those local computers.

Public IP addresses allow anyone on the Internet to connect directly to a computer, barring any firewalls or other blocks in place, but private IP addresses are specifically non-routable without a bit of extra work.

You can also access your base station remotely for file sharing and configuration using an iCloud account and Back to My Mac.

Know Your Options

You can choose from several different methods of reaching your network from the outside world:

- **Basic port mapping and reserved addressing:** While earlier Apple base stations offered *port mapping*, a way to connect a public port on a routable address on the base station with a private port on a locally connected computer, 802.11n and ac base stations also let you assign addresses to local computers on a persistent basis—these *reserved* addresses don't change over time. When the base station is restarted, or when the computer is restarted, the same address is assigned to the computer once again.

This reservation system makes the mapping system work consistently with less effort. I cover how to map ports for remote access just ahead after this list.

- **Punch through from certain programs:** A protocol from Apple called *NAT-PMP* (NAT plus Port Mapping Protocol) helps

with port mapping without requiring any special configuration on a computer or a base station. This option works only when the software you're using is aware of NAT-PMP and can talk to the base station using this protocol, and when you have a publicly reachable IP address assigned to your base station. You can find out more in [Punch Through with NAT-PMP](#).

- **Use one computer as your default host:** There's a coarser way to make NAT work, too, allowing a single computer behind the NAT gateway to act as though it's directly connected to the Internet. This option is appropriate in limited cases where you want a machine to be reachable from the Internet on any of its ports without getting publicly reachable IP addresses from your ISP for computers on your network. I describe this default host option in [Set a Default Host for Full Access](#).
- **Configure and monitor your base station and mount attached disks via Back to My Mac:** If you have an iCloud account, you can access your base station remotely via AirPort Utility for Mac in 10.7 Lion or later. Once you've accessed it, you can reconfigure it or mount any internal (Time Capsule) or USB-attached disks. I provide directions in [Access a Base Station via iCloud](#).

Map Ports for Remote Access

Port mapping relies on network address translation (NAT). NAT acts as a gateway between a WAN IP address for a router reachable from a larger LAN or the public Internet, and the private addresses hidden behind NAT on the base station's LAN.

NAT Maps Private to Public Connections

When a computer within the LAN wants to connect to the Internet, the NAT software creates an association between that computer's outgoing connection and a public port on the WAN IP address of the base station. (I talk more about [Ports](#) in the sidebar slightly ahead.)

Set Up a Shared Printer

With a base station set up to handle local computers and hooked into the Internet, your next step may be to attach a printer to the base station so that it can be shared among all the local computers. In this chapter, I explain how to set up a base station for an attached printer using either a USB or a wireless connection, and how [Add a Shared Printer in Mac OS X](#) and [Add a Shared Printer in Windows](#).

Add a Printer with USB

Plug the printer into the base station (any AirPort model) or a USB hub (Extreme, Time Capsule). You should not need to reboot your base station for it to recognize the printer.

The AirPort Extreme and the Time Capsule each have a lone USB port that can connect to either a single printer or a single hard drive. Add a USB hub, and you can connect one or more printers and drives in any combination. (For maximum reliability and performance, I recommend a Hi-Speed powered hub with external AC power.) The AirPort Express is designed to connect to only a single USB printer, but not to an attached hard drive nor a hub.

Add a Wi-Fi Printer Using WPS

An option added in a base station firmware update in 2013 makes it easier to add Wi-Fi-enabled printers that support Wi-Fi Protected Setup (WPS) to an AirPort network. WPS lets a device join a network securely once you tell the base station that the device wants to connect.

Before starting, check whether your printer has a PIN (this will be in the manual) or if it can connect automatically to any base station in range that offers a connection.

To make the connection:

1. Select a base station in AirPort Utility for Mac.
2. Choose Base Station > Add WPS Printer.
3. In the Add WPS Printer dialog (**Figure 79**), select PIN if your printer has a PIN or First Attempt if it will accept any available network. Click Continue.



Figure 79: The Add WPS Printer dialog lets you pick how to connect a WPS printer to the network.

4. Depending on what you selected, you will see:
 - **PIN:** Enter the PIN provided, and click Continue.
 - **First attempt:** A dialog with a waiting spinner appears until the printer connects.
 5. You may need to select the network from a menu on the printer.
- If the connection is made, the printer will be available on the network.

Add a Shared Printer in Mac OS X

To add a shared printer to a Mac, make sure the printer is on and not in standby-power mode, and then use these steps:

1. Open the Printers & Scanners system preference pane.

Note: These steps work specifically in 10.9 Mavericks, but they should work okay back through 10.5 Leopard.

Set Up a Shared USB Disk

The AirPort Extreme and the Time Capsule both add an interesting option to a network: they can share disks across a network without those disks being attached to a computer. Both models can accept one or more external drives plugged in via USB or via a USB hub; the Time Capsule also includes a non-removable internal drive.

Either model can share drives over a network with both the standard *Apple Filing Protocol* (AFP) format, the same format used with Personal File Sharing and OS X Server share files, and *Samba*, a network file-sharing service compatible with Mac OS X, Windows, and Linux.

Attached hard drives can be accessed over the Internet via AFP using Back to My Mac, too (see [Access a Base Station via iCloud](#)).

In this chapter, I cover a handful of procedures for using the Time Capsule and the Extreme to share disks:

- Read [Prepare Your Drive](#), next, to find out about formatting and physically attaching drives.
- [Work with Time Machine](#) covers setting up Time Machine backups as well as how to make a backup archive of a Time Capsule disk or to erase the disk.
- [Grant Access](#) and [Gain Access](#) look at how users on the network can best access the disks.

Warning! You can't share volumes via either only AFP or only Samba; you must share through both.

Prepare Your Drive

The Time Capsule's internal drive comes preformatted, so it should be ready to go, but it can be erased to its pristine state through AirPort Utility (see [Erase](#), ahead).

You must format attachable disks before you connect them to the base station, using either the Mac HFS+ format, or the FAT16 or FAT32 (MS-DOS) formats. Each partition on a disk becomes a separately available shared volume. (FAT16 supports smaller maximum partition sizes than FAT32; you're unlikely to see FAT16 except on disks formatted by very old computers.)

You can connect a single drive to the USB port on the Extreme or Time Capsule, or connect a USB hub and then a series of drives to the hub. The drives may be hard drives or USB thumb (flash) drives, but you cannot use CD/DVD drives with removable media.

Once one or more drives are formatted and connected, you can access them and let others access them, too. You handle all the limited configuration options in AirPort Utility in the Disks view.

Share Files with AirDrop

Have you ever wanted to swap a file between a couple of your own computers without setting up file sharing and mounting a volume? Or pass a file to a friend or colleague without joining a common Wi-Fi network, setting up ad-hoc networking, or emailing it?

AirDrop is a solution to that common problem. Added in 10.7 Lion, the feature lets you find and share files with other users near you. It has a pile of provisos that I discuss below, but it's a remarkably nifty way—when the right hardware is available—to hand files back and forth.

Note: AirDrop for iOS works on the iPhone 5 and later, 4th-generation iPad, iPad Air, iPad mini, and 5th-generation iPod touch or later. (It also requires an iCloud account to access your contacts.) I've never made it work between two iOS 7 devices, and no troubleshooting from Apple has helped. My editor, Tonya Engst, reports success with using AirDrop between an iPhone 5S and 5.

What Makes AirDrop Tick

AirDrop for Mac relies on a special feature in new Wi-Fi adapters that allows a network card to connect simultaneously to a Wi-Fi network and to other devices on a peer-to-peer basis. A Wi-Fi network is typically called an *infrastructure* network, as it provides a hub around which all network activity zooms. In contrast, a peer-to-peer network is known as a *personal area network (PAN)* network; it allows direct communication among devices without a central coordinating switch.

This sounds a lot like [Ad Hoc Networking](#), doesn't it? With *ad hoc* or *computer-to-computer* networking, a set of computers can all connect to one another as peers. However, ad hoc networking has three drawbacks. First, it doesn't include robust security, and even the available security requires each party to type in an encryption key. Second, you can't maintain a connection to an Internet-connected

base station network and use ad hoc networking at the same time. And, finally, you still have to establish a file-sharing connection on top of the ad hoc network.

AirDrop eliminates all that. Click a button in the Finder, and an AirDrop window opens showing all available peers in the vicinity. Drop a file (or files) into the AirDrop window, and it's done. The process is equally simple on the receiving end.

You can use AirDrop only with other computers that are running Lion or later, and those computers must have a fairly recent vintage Wi-Fi chipset (a range of models starting in 2008 to 2010). Wi-Fi must be active for it to work. (Apple has a list of minimum Mac models [in a support note](#).)

Note: Apple has announced that iOS 8 and Yosemite will allow AirDrop to work among Macs and iOS devices. Until both OS updates are released, it is limited to Mac-to-Mac or iOS-to-iOS transfers.

Note: AirDrop for iOS and OS X both require Bluetooth be enabled, as it uses Bluetooth as a low-power way to pass connection information.

Transfer Files with AirDrop

To use AirDrop for iOS 7, swipe up from the bottom of the screen to open the Control Center; in the Control Center, turn on Wi-Fi, Bluetooth, and AirDrop; and then look for AirDrop as an option when you share something, such as a photo. You can find full directions in Apple's [Use AirDrop to wirelessly share content](#) article.

Transferring files with AirDrop on a Mac is a breeze:

1. In any Finder window, in the top of the sidebar under Favorites, click AirDrop (**Figure 89**). This item appears only if your system is capable of using AirDrop as noted just above, but if you don't see

Secure Your Network

If you use a wired network in your home, someone would have to break into your house, plug into your Ethernet switch, and then crouch there in the dark to capture data passing over your network.

Wireless networks have no such protection: anyone with an antenna sensitive enough to pick up your radio signals can eavesdrop on traffic passing over your network. This could be a neighbor, someone in a parked car, or a nearby business. Many free, easy-to-use programs make this a simple task for only slightly sophisticated snoopers.

However, you're not powerless to prevent such behavior. Depending on what you want to protect and whom you're protecting against, you can close security holes with tools that range from a few settings up to industrial-grade protection that requires separate servers elsewhere on the Internet.

Simple Tricks That Don't Work

You may have read suggestions for setting up basic security that advise you to hide your network's name and make it hard to connect to. In practice, this doesn't work.

In a closed network, your base station stops broadcasting its network name, or SSID (Service Set Identifier), as part of its *beacon*, an "I'm here" message that access points regularly transmit in order to help clients connect to them. However, the beacon continues to be sent because it still includes information that is used for network data synchronization.

An open network appears by name in the Wi-Fi  menu or in other places in a device's interface that show the names of networks you can connect to. But closing the network makes it only slightly obscure. A cracker can easily find out that the network exists, and by monitoring for a connection or using a tool to create a *disassociation*

for a computer on the network—which forces that computer to reconnect—the cracker can grab the network’s name. So you cannot rely on closing your network for any real security.

Although I discourage bothering with a closed network, here’s how to set one up:

1. In AirPort Utility (Mac or iOS), select and edit your base station, and then:
 - **On a Mac:** Click the Wireless button and then the Wireless Options button; then select the Create Hidden Network checkbox.
 - **In iOS:** Tap Network, and then turn on the Hidden Network switch.
2. Update the base station:
 - **On a Mac:** Click Save and then click Update.
 - **In iOS:** Tap Done repeatedly to reverse through a few configuration screens and then tap Update.
3. Wait for the base station to reboot.

Timed Access Control

Apple used to offer a way to limit access to devices by their MAC address, a unique identifier set for every network adapter. While this feature was removed, AirPort Utility does retain Timed Access Control (in the Network view) to limit devices to access the network on specific days of the week during specific hour ranges. You set access for a device by its MAC address (see [Appendix D: What and Where Is a MAC Address?](#)).

The feature can be useful if you’re trying to keep your kids (or spouse?) from using the Internet except during certain hours, but I find that it is too fussy to recommend, and the same settings must be re-entered on every base station on a network. It also doesn’t restrict plugging in via Ethernet.

Overcome Interference

A frustrating part of Wi-Fi networking is that you can't control your "air space." All too often, neighboring Wi-Fi networks and other emitters cause reception problems in areas that otherwise would have good reception. If your network's performance varies by time of day or even by the minute, the ideas in this chapter may help you identify the problem.

Do Some Basic Testing

What you test for varies by band. Keep reading after the tests for some suggestions for how to fix found problems.

For 2.4 or 5 GHz:

- Run [iStumbler](#) to determine whether other networks are running nearby. iStumbler scans for networks and can display their characteristics, such as signal strength and whether security is enabled. It can't tell you more general info about signals being generated in the spectrum range, however.
- If you're desperate for a solution, check out Wi-Spy, a relatively inexpensive spectrum analyzer that comes in 2.4 GHz only and 2.4 and 5 GHz versions. It can show whether there's interference beyond Wi-Fi. (See [Testing from Client to Base Station](#).)

For 2.4 GHz only:

- Investigate your cordless phones and microwave oven as culprits—they can both create static on the Wi-Fi line. Do you have problems only when talking on the phone or making popcorn? There you go.
- Is your Wi-Fi network near a hospital, or light or heavy industry? Some medical and industrial devices use the 2.4 GHz band, including microwave sealers that close bags of potato chips. You might need to use wired Ethernet or upgrade to computers that can use the 5 GHz band to overcome that problem.

For 5 GHz:

- Check whether you have 5.8 GHz cordless phones.
- See whether a wireless ISP might be broadcasting over 5 GHz in your area. Most wISPs are using the 5.8 GHz section of the 5 GHz band. (If that's the case note the second bullet item in the solutions for cordless phones, below.)

Try a Solution

Here are ideas for solving some of the problems noted just previously.

If cordless phones are the culprit:

- Buy new cordless phones that use a band that doesn't interfere with your Wi-Fi network. The popular DECT standard finally entered the United States a few years ago in its DECT6 version, which relies on 1.9 GHz signals. You can also find 5.8 GHz cordless phones.
- In 5 GHz, use lower-numbered channels; 5.8 GHz falls within the highest range of channels supported by 802.11n base stations. (This solution also reduces interference from wireless ISPs, firms that use 5 GHz to provide residential Internet service.) Using a lower-numbered channel will reduce the signal strength of your network by 95 percent, but it might be the only solution in extreme cases.

If a neighboring network is causing the problem:

- Propose an informal channel usage agreement: if your neighbor and you are both using 2.4 GHz's channel 6, switch to 1 and 11 to increase the distance between signals. In 5 GHz, you have a number of additional channels to choose from.
- You (and your neighbor) could move your access points farther away from one another to reduce the signal conflict in the middle.

Appendix A:

Configuration Files

You can export the current state of your base station configuration to a file that can be imported later, to the same base station or to a different one. This is useful when you want to create a model configuration with the same network name, password, and other details, and then use it to configure many base stations.

To export a configuration:

1. In AirPort Utility for Mac, select the base station and click Edit.
2. Choose File > Export Configuration File, and name the file descriptively, as there will be few other clues that help you identify the file.

If you want to restore a base station to the settings in a file or configure a different base station in the same way, follow these steps to import the exported configuration file:

Warning! Before importing a configuration, you should save a copy of your current active setup using the steps given just previously. Importing overwrites your current active base station settings.

1. In AirPort Utility for Mac, select the base station and click Edit.
2. Choose File > Import Configuration File.
3. Select the configuration file, and click Open.

AirPort Utility asks which settings in the configuration file you'd like to import (**Figure 96**). If a type of setting isn't configured, no checkbox shows for that item, logically enough. Base stations allow timed settings, which can restrict access to given computers at given times of the day or week; port mapping rules for allowing inbound

access to local computers; DHCP reservations for assigning addresses to local computers; and miscellaneous other settings.



Figure 96: Select settings to import.

4. Select the options you want to import, and click OK.
5. Click Update to apply the imported profile's settings.

Once the file is imported, the settings replace your current base station settings.

Tip: Importing just items like Timed Access Control or DHCP Reservations lets you transfer just those settings among multiple base stations after you update them on one base station without resetting the other base stations' names or assigned IP addresses.

Appendix B: Setting up a Software Base Station

You can use a Mac equipped with a Wi-Fi adapter card not just as a client on a Wi-Fi network, but also as a base station. In this appendix, I explain how to set up a software base station in 10.5 Leopard and later, as well as how to use [Ad Hoc Networking](#), which has some elements in common with software base stations.

Software Base Station or Ad Hoc Network?

A *software base station* walks and talks like a base station: it puts out the same kind of messages that other computers recognize from a base station. You need at least two network interfaces to turn on a software base station: a Wi-Fi adapter plus some other interface, like an Ethernet network connection.

Ad hoc networking is a computer-to-computer mode, and it doesn't require a second adapter to reach another network, although it can handle that. Ad hoc can be used sometimes by simpler devices. An ad hoc network can't use modern WPA2 security, because that method requires a central hub to manage the encryption process.

Most operating systems distinguish between ad hoc networks (which are sometimes seen as more risky) and base stations. The fact that you can create software base stations eliminates the risk distinction; crackers use software base-station programs to lure hotspot users, for instance.

Software Base Station

The software base station is a breeze to set up: pick a channel, set security (which I recommend), and turn it on. Let me explain your tradeoffs for channel choices and security first, however.

Frequency

10.7 Lion was the first release of Mac OS X that allows you to select either a 2.4 GHz or 5 GHz channel for use with a software base station. You can pick any 2.4 GHz channel, as well as 5 GHz channels 36, 40, 44, and 48. (These channels vary by country.) Apple is offering only 4 of the 8 channels available in its dedicated base stations, which are just 8 of the 23 legal channels in the United States. These lower-numbered channels (36, 40, 44, and 48) broadcast at no more than 5 percent of the maximum legal power of the higher-numbered channels according to U.S. rules. Apple must have thought it better to use lower power and thus not interfere with any nearby networks (read [Channels](#) for more).

Security

After years of providing lackluster security for the software base station, Apple finally upgraded it with the release of 10.8 Mountain Lion (and didn't advertise the fact). Mountain Lion offers WPA2 Personal security, which provides the highest degree of security available. WPA2 Personal replaced the older WEP encryption, which I described back in [Use Built-in Encryption](#), in 2004. (WEP remains the only option in Lion, however.)

The other advantage of WPA2 Personal is that it's compatible with 802.11n as well as with 802.11ac. WEP can work only with 802.11g (2.4 GHz) and 802.11a (5 GHz), thus reducing your software base station's throughput.

In Mountain Lion and later, as you follow the steps ahead for turning on a software base station, you'll be able to choose None or WPA2 Personal as the security method. None will let anyone join, of course, while WPA2 Personal requires that other devices have the passphrase you set. Nearly every piece of hardware labeled "Wi-Fi" shipped since 2004 (and some from 2003) can work with WPA2 Personal security.

Appendix C:

Channels Explained

The ins and outs of channels used in each band have wound up in this appendix, as you may need to know the details only when something goes wrong—or you may be among the more technically inclined readers who want to know more about the technical minutiae of Wi-Fi. In this appendix, you can learn about why the 2.4 and 5 GHz channels are organized the way they are, and what happened to 15 missing 5 GHz channels.

Channels in 2.4 and 5 GHz are 20 MHz wide; an optional 40 MHz wide, or double-channel, option was added in 802.11n, although Apple allows 40 MHz wide channels only in 5 GHz. 802.11ac expanded this to 80 MHz and 160 MHz wide channels; Apple included the mandatory 80 MHz width, but not the optional 160 MHz addition. The two bands have different ways of defining and making those channels available.

Channel availability varies from country to country. Apple lists which channels it supports in the [technical specs for its base stations](#). You can also see a [table of 5 GHz channels worldwide](#) in Wikipedia.

MHz and Mbps

Megahertz does, in fact, correlate to megabits per second. *Shannon's Law* (or the Shannon-Hartley Theorem), a bit of information theory, says that there's a direct relationship that ties the width of a channel and the ratio of signal to noise to the achievable data rate. Twice the channel width means up to twice the raw data (**Figure 102**).

$$C = B \log_2 \left(1 + \frac{S}{N} \right)$$

Figure 102: *Shannon's Law (image via Wikipedia).*

In case you were wondering, the formula is: maximum bit rate equals channel width in hertz multiplied by log2 of the sum of 1 + signal divided by noise.

See [Pick Compatibility and Set a Channel](#), earlier, to learn how to set your base station's channel in AirPort Utility.

2.4 GHz Channels

In the United States, 802.11 standards can use any of 11 numbered, staggered channels in the 2.4 GHz band (**Figure 103**). Because these channels are staggered and overlap, only channels 1, 6, and 11 in the United States can be used in networks that overlap their coverage area, assuming you want the least interference. (In some countries, the 2.4 GHz band is slightly wider, allowing for four non-overlapping channels.)

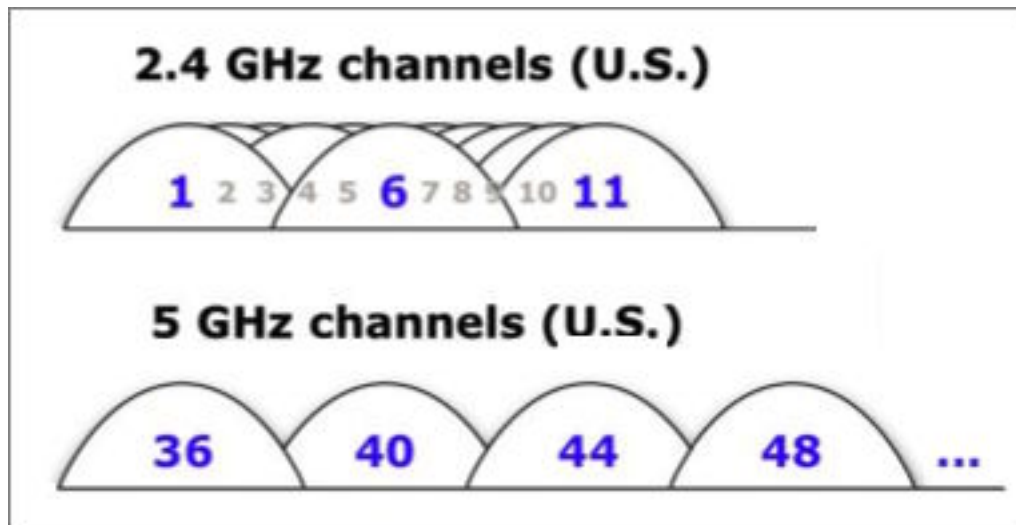


Figure 103: 2.4 GHz 802.11 channels are staggered, with channels 1, 6, and 11 having the least overlap. 5 GHz 802.11 channels have little overlap; only the four lowest channels of 23 are shown.

All 2.4 GHz channels have the same power limits, but there's a distinct difference in the permitted level of signal strength—which affects the distance at which Wi-Fi can work and the top speeds available.

Also, due to the overlapping, staggered nature of the channels, there is room in 2.4 GHz for only a single unique 40 MHz channel and a single 20 MHz channel to be used at the same time—and then only in ideal cases. This is why Apple didn't want wide channels in 2.4 GHz.

Appendix D: What and Where Is a MAC Address?

The MAC, or *Media Access Control*, address is a unique, factory-assigned address for every Ethernet and Wi-Fi adapter. A MAC address consists of six two-digit hexadecimal numbers separated by colons, such as 0C:F2:33:01:02:FC. (*Hexadecimal*, or *hex*, is the base 16 number system, with values running from 0 to 9, and then from A to F for 10 to 15.) The first three numbers are assigned to a manufacturer by a coordinating association; Apple has at least two common ranges, which begin with 00:0a:95 and 00:03:93. MAC addresses are often used for filtering, authentication, and WDS, often without requiring direct entry.

Some routers from other makers can have their MAC address changed in a process called *MAC cloning* or *spoofing*, which is sometimes useful when you have to register a computer's MAC address, but then want to use a router in its place. No Apple base station has ever offered this capability, although Mac OS X allows it for Macintoshes via a Terminal command.

Here are various ways to locate Mac addresses:

From a base station:

For a base station that pre-dates the 2013 802.11ac models, look on the bottom of the unit.

- The *AirPort ID* or *Wi-Fi ID* is the wireless MAC address. From 2009 to 2012, all models of the Extreme and Time Capsule as well as the 2012 Express have two AirPort IDs, one for each band's radio, and they are noted by band on the base station.
- The *Ethernet ID* is the WAN port's MAC address.

Or in AirPort Utility for Mac, select a base station and hover over the network's name, as in **Figure 104**.



Figure 104: View the base station's MAC addresses by hovering over the name.

Or in AirPort Utility for iOS, select the base station icon and then tap Hardware Info.

Devices connected to a base station via Wi-Fi:

In AirPort Utility for Mac, select the base station and hover over a connected device's name in the Wireless Clients list (**Figure 105**). The Name shows either the value entered in the Network preference pane in Mac OS X or a Bonjour name.

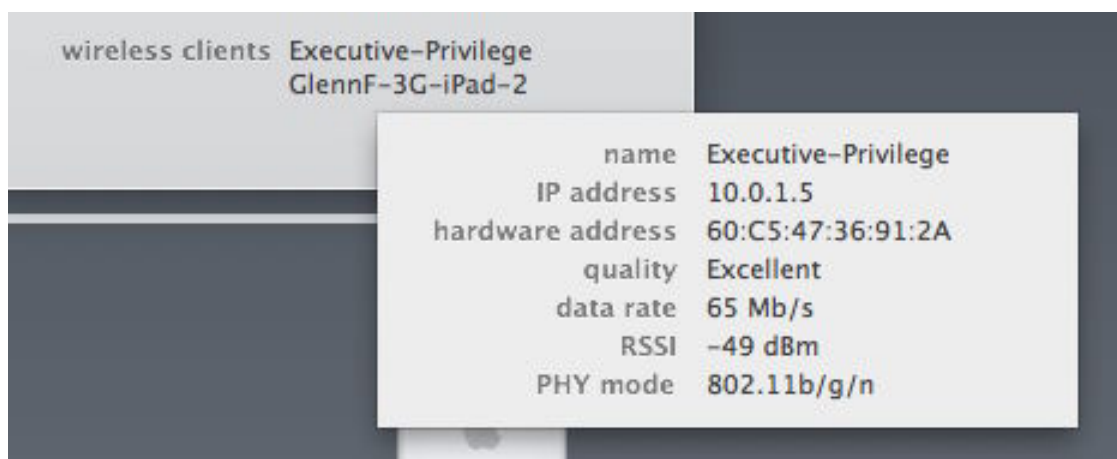


Figure 105: Wireless Clients reveal information about connected devices when you hover over a name in the list.

Wi-Fi adapter in a Mac:

In Mac OS X, open the Network System Preferences pane. Click Wi-Fi in the adapter list, and click the Advanced button. The MAC number is the Wi-Fi Address. (Leopard and Snow Leopard call this the AirPort ID.)

About This Book

Thank you for purchasing this Take Control book. We hope you find it both useful and enjoyable to read. We welcome your [comments](#).

Ebook Extras

You can [access extras related to this ebook](#) on the Web. Once you're on the ebook's Take Control Extras page, you can:

- Download any available new version of the ebook for free, or buy a subsequent edition at a discount.
- Download various formats, including PDF, EPUB, and Mobipocket. (Learn about reading on mobile devices on our [Device Advice](#) page.)
- Read postings to the ebook's blog. These may include new information and tips, as well as links to author interviews. At the top of the blog, you can also see any update plans for the ebook.

If you bought this ebook from the Take Control Web site, it has been automatically added to your account, where you can download it in other formats and access any future updates. However, if you bought this ebook elsewhere, you can add it to your account manually:

- If you already have a Take Control account, log in to your account, and then click the “access extras...” link above.
- If you don't have a Take Control account, first make one by following the directions that appear when you click the “access extras...” link above. Then, once you are logged in to your new account, add your ebook by clicking the “access extras...” link a second time.

Note: If you try these directions and find that your device is incompatible with the Take Control Web site, [contact us](#).

About the Author



Glenn Fleishman is owner and editor of [The Magazine](#), a fortnightly subscriber-supported, ad-free electronic periodical for curious people with a technical bent. He hosts a podcast about fundamental changes in the economy of making art and making things, [The New Disruptors](#). Glenn also writes for the [Economist's Babbage blog](#), and he is a regular contributor to the publication's print edition. He can be heard regularly on public radio in Seattle and nationwide, as well as on the podcast [The Incomparable](#).

He lives in Seattle in a bungalow with his wife and two sons. His older child's first word was "book," not "Mac."

Acknowledgments

I want to thank Tonya Engst for her continued work in developing this book through now its fourth major overhaul, and her attention to detail as we fiddle with the fine points. Adam Engst also continues to help improve this title through brainstorming and great feedback.

Thanks to Ed Bott for his work in providing Windows 8.1 directions and screen captures. You can find Ed on Twitter at [@edbott](#) or at his [Real-world Windows and Office Web site](#).

About the Publisher

Publishers Adam and Tonya Engst have been creating Apple-related content since they started the online newsletter [TidBITS](#) in 1990. In TidBITS, you can find the latest Apple news, plus read reviews, opinions, and more.

Adam and Tonya are known in the Apple world as writers, editors, and speakers. They are also parents to Tristan, who has reached the age where he can read, understand, and find mistakes in the Take Control series.



Credits

- Publisher: Adam Engst
- Editor in Chief: Tonya Engst
- Editor: Tonya Engst
- Production Assistants: Michael E. Cohen, Oliver Habicht
- Cover design: Sam Schick of [Neversink](#)
- Logo design: Geoff Allen of [FUN is OK](#)

Copyright and Fine Print

Take Control of Your Apple Wi-Fi Network

ISBN: 978-1-61542-438-2

Copyright © 2014, Glenn Fleishman. All rights reserved.

[TidBITS Publishing Inc.](#)

50 Hickory Road

Ithaca, NY 14850 USA

Take Control electronic books help readers regain a measure of control in an oftentimes out-of-control universe. Take Control ebooks also streamline the publication process so that information about quickly changing technical topics can be published while it's still relevant and accurate.

This electronic book doesn't use copy protection because copy protection makes life harder for everyone. So we ask a favor of our readers. If you want to share your copy of this ebook with a friend, please do so as you would a physical book, meaning that if your friend uses it regularly, he or she should buy a copy. Your support makes it possible for future Take Control ebooks to hit the Internet long before you'd find the same information in a printed book. Plus, if you buy the ebook, you're entitled to any free updates that become available.

You have our permission to make a single print copy of this ebook for personal use. Please reference this page if a print service refuses to print the ebook for copyright reasons.

Although the author and TidBITS Publishing Inc. have made a reasonable effort to ensure the accuracy of the information herein, they assume no responsibility for errors or omissions. The information in this ebook is distributed "As Is," without warranty of any kind. Neither TidBITS Publishing Inc. nor the author shall be liable to any person or entity for any special, indirect, incidental, or consequential damages, including without limitation lost revenues or lost profits, that may result (or that are alleged to result) from the use of these materials. In other words, use this information at your own risk.

Many of the designations used to distinguish products and services are claimed as trademarks or service marks. Any trademarks, service marks, product names, or named features that appear in this title are assumed to be the property of their respective owners. All product names and services are used in an editorial fashion only, with no intention of infringement of the trademark. No such use, or the use of any trade name, is meant to convey endorsement or other affiliation with this title.

This title is an independent publication and has not been authorized, sponsored, or otherwise approved by Apple Inc. Because of the nature of this title, it uses terms that are the trademarks or that are the registered trademarks of Apple Inc.; you can view a [complete list](#) of the trademarks and of the registered trademarks of Apple Inc.

Featured Titles

Click any book title below or [visit our Web catalog](#) to add more ebooks to your Take Control collection!

[*Take Control of 1Password*](#) (Joe Kissell): Slowed down by entering passwords repeatedly? Learn how to let 1Password do the heavy lifting.

[*Take Control of Apple TV*](#) (Josh Centers): This essential guide covers everything you need to know about the Apple TV!

[*Take Control of Backing Up Your Mac*](#) (Joe Kissell): Set up a rock-solid backup strategy so that you can restore quickly and completely, no matter what catastrophe arises.

[*Take Control of CrashPlan Backups*](#) (Joe Kissell): Find expert real-world advice about CrashPlan's onsite, offsite, and cloud backups.

[*Take Control of iBooks Author*](#) (Michael E. Cohen): Plan your project, customize a template, set up a table of contents, lay out pages, add interactivity and glossary items, and publish your masterpiece!

[*Take Control of iCloud*](#) (Joe Kissell): Understand the many features, get set up properly, and enjoy iCloud!

[*Take Control of iTunes 11: The FAQ*](#) (Kirk McElhearn): Wrap iTunes around your little finger and enjoy your media more.

[*Take Control of the Cloud*](#) (Joe Kissell): Cut through the hype, understand cloud services, and enhance your privacy and security!

[*Take Control of the Mac Command Line with Terminal*](#) (Joe Kissell): Learn the basics of the Unix command line that underlies Mac OS X, and get comfortable and confident when working in Terminal.

[*Take Control of Your Paperless Office*](#) (Joe Kissell): With your Mac, scanner, and this ebook in hand, you'll finally clear the chaos of an office overflowing with paper.